CITY OF SAN ANTONIO

OFFICE OF THE CITY AUDITOR

Audit of Information Technology Services Department
Configuration Management

Project No. AU10-012

September 1, 2011

Executive Summary

As part of our annual Audit Plan approved by City Council, we conducted an Information Technology Services Department (ITSD) configuration management audit. This audit is the third in a series of audits we will perform over the next few years to assist ITSD by evaluating information technology general controls that apply to all or a large segment of the City's computer applications (see **Appendix B** on page 5 for our tentative IT audit schedule). The audit objective and conclusion follow:

> ***Determine if changes to information technology resources are authorized and systems are configured and operating securely*.**

We determined that changes to information technology resources are authorized and systems are configured and operating securely with respect to change management.

ITSD has developed and consistently followed a configuration management (a.k.a. change management) process that includes planning, impact analysis, and a formal approval process that includes a Change Approval Board. Furthermore, the system development process is well documented and considers security controls throughout the lifecycle.

Management of ITSD agrees with the audit report. Its verbatim response is in Appendix D on page 7.

Table of Contents

Background

Information Technology (IT) systems play a vital role in acquiring, processing, storing and distributing key financial, operational, and human resource related data at the City of San Antonio. ITSD provides IT services to all City Departments, delegate agencies, various local, state, and federal government entities through information and technology sharing agreements.[1]

ITSD is structured as a centralized IT shared services organization that provides governance and support for all technology functions and builds information systems around IT industry practices that facilitate the goals and objectives of the City of San Antonio.

ITSD is comprised of four areas, Enterprise Application Support, Enterprise Information Technology Infrastructure, Public Safety, and Customer Relations.

One of the 11 Goals and Objectives of ITSD is Customer Support Services. Their mission is to provide an improved single point of contact for IT Support 24-hours a day, 7-days a week that will improve the business processes for customer service, *asset management, inventory, change management* and incident management. The Service Desk provides two separate and distinct functions: *(1) logging, tracking, resolution, and elevation of problems; and (2) coordination of all data and voice service requests for adds, moves, and changes.*[2]

Configuration management (CM) provides reasonable assurance that changes to information system resources are authorized, tested, and tracked, and that systems are configured and operating securely and as intended. CM also entails updating software on a timely basis to protect against known vulnerabilities.

In October 2010, ITSD implemented a CM software solution called BMC Remedy for facilitating configuration changes. BMC Remedy applies a repeatable process for information system changes to improve the stability of business service and required technology configuration changes. BMC Remedy facilitates change requests and approval, risk analysis, planning, orchestration of tasks, verification, and change tracking. Additionally, BMC Remedy can manage and track IT related assets such as mobile devices, security cameras, handheld radios, computers, network equipment, software and applications.

[1] City of San Antonio, Texas*, Balanced Adopted Annual Operating and Capital Budget - Fiscal Year 2011*, (San Antonio, 2010), 508.
[2] Ibid.

Audit Scope and Methodology

The audit scope included FY 2011 (October 1, 2010 through the present). The audit included inquiries of City ITSD employees and review of documented policies and procedures provided by ITSD management. Furthermore, auditors utilized BMC Remedy to review configurable item[3] change details.

Our audit also included tests of management controls that we considered necessary under the circumstances. These tests verified that the Change Approval Board was operating effectively and included appropriate representation across the entity. Additionally, auditors verified that information technology hardware and software items are inventoried and mapped to the application(s) they support.

Auditors tested samples of system changes, normal and emergency, to determine that the organization uses a systematic process that includes justification, review, impact analysis and approval. Auditors also reviewed policies and procedures pertaining to version controls and verified that access controls surrounding the source code library exist and are effective.

Other policies and procedures reviewed pertain to infrastructure maintenance, patch management, troubleshooting, and hardware reconciliations. Auditors also verified that policies and procedures are in place surrounding application development and include an effective System Development Life Cycle.

We obtained sufficient criteria and best practices for Information Technology (IT) related processes and procedures. We used the Government Accountability Office's (GAO) Federal Information System Controls Audit Manual (FISCAM). FISCAM presents a methodology for performing information system control audits in accordance with government auditing standards. We also relied on related National Institute of Standards and Technology (NIST) security publications.

We conducted this audit from January 2011 to June 2011 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate information to provide a reasonable basis for the results based on the audit objectives. We believe that the information obtained provides a reasonable basis for our audit results and conclusions based on our audit objectives.

[3] Hardware, software, relationships, documentation, personnel attributes, etc.

Internal Controls

Based on the Control Objectives for Information and related Technology (COBIT) maturity model for managing changes[4], we concluded that overall, the maturity of ITSD's change management process is at the "Defined Process *(3)*" level but approaching the "Managed and Measurable (4)" level.

ITSD's change management process is a formal process that includes categorization, prioritization, emergency procedures, change authorization and release management. Additionally, change management documentation is current and correct, with changes formally tracked and auditable in the BMC Remedy Change Management System.

Maturity modeling is a method of evaluating internal controls in their current state against a maturity scale of non-existent (0) to optimized (5). The ultimate or target maturity level should be higher (e.g. 3, 4, or 5) rather than lower and should be influenced by ITSD and COSA business objectives, dependence on IT, technology sophistication, and most importantly, the value of the City's information. Additional explanations of the different levels of the COBIT maturity model are included in **Appendix A** on page 4.

[4] IT Governance Institute – COBIT 4.1, *AI6 – Acquisition and Implementation – Manage Changes*, 96.

Appendix A – COBIT Maturity Model

The COBIT maturity model for managing changes[5] is based on six levels of maturity, which are paraphrased below:

0 Non-Existent: There is no defined change management process, and changes can be made with virtually no control. There is no awareness that change can be disruptive for IT and business operations, and no awareness of the benefits of good change management.

1 Initial: It is recognized that changes should be managed and controlled. Practices vary, and it is likely that unauthorized changes take place. There is poor or non-existent documentation of change and configuration documentation is incomplete and unreliable.

2 Repeatable but Intuitive: There is an informal change management process in place and most changes follow this approach; however, it is unstructured, rudimentary and prone to error. Configuration documentation accuracy is inconsistent, and only limited planning and impact assessment take place prior to a change.

3 Defined Process: There is a defined formal change management process in place, including categorization, prioritization, emergency procedures, change authorization and release management, and compliance is emerging. Workarounds take place, and processes are often bypassed. Errors may occur and unauthorized changes occasionally occur.

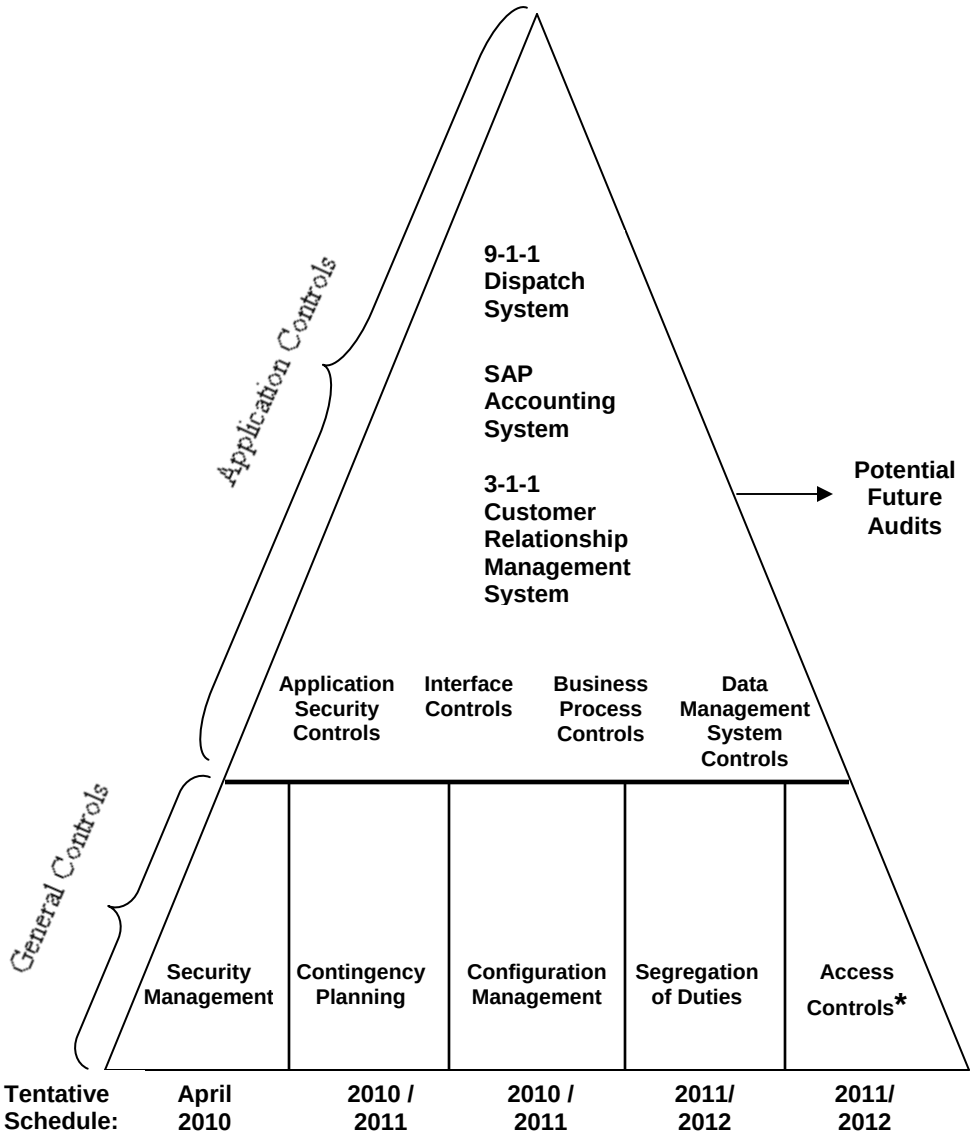
4 Managed and Measurable: The change management process is well developed and consistently followed for all changes, and management is confident that there are minimal exceptions. The process is efficient and effective, but relies on considerable manual procedures and controls to ensure that quality is achieved. All changes are subject to thorough planning and impact assessment to minimize the likelihood of post-production problems. An approval process for changes is in place. Change management documentation is current and correct, with changes formally tracked.

5 Optimized: The change management process is regularly reviewed and updated to stay in line with good practices. The review process reflects the outcome of monitoring. Configuration information is computer-based and provides version control.

[5] Ibid.

Appendix B – Information Technology Audit Schedule

Based on FISCAM Control Categories



*Access Controls include physical access security (e.g. data center access) and logical access security audits. Logical access security may include audits of system-level components such as the City's IT network (e.g. firewalls, web servers, routers), operating systems (server and workstation), and infrastructure application software (e.g. database management systems, identification and authentication systems, email/messaging systems, etc.).

Appendix C – Staff Acknowledgement

Mark Bigler, CPA-Utah, CISA, CFE, Audit Manager
Gabe Trevino, CISA, Auditor in Charge

Appendix D – Management Response

CITY OF SAN ANTONIO
SAN ANTONIO TEXAS 78283-3966

Kevin W. Barthold, CPA, CIA, CISA
Acting City Auditor
San Antonio, Texas

RE: Management's Acknowledgement of Information Technology Services Department Configuration Management Audit

Here are our comments to the subject report.

☑ Fully Agree (provide detailed comments)

☐ Agree Except For (provide detailed comments)

☐ Do Not Agree (provide detailed comments)

Sincerely,

Hugh Miller
Chief, Technology Officer/Director
Information Technology Services Department

Ben Gorzell
Chief Financial Officer
City Manager's Office